Datum
2024-04-02

Vår beteckning
FK 2024/002297

Svar på regeringsuppdrag

Informationssäkerhet

Försäkringskassan

Informationssäkerhet på Försäkringskassan

Försäkringskassan har fått i uppdrag att redogöra för hur myndigheten arbetat för att förvalta och utveckla sin informationssäkerhet och för hur myndigheten planerar för att möta framtida behov. Försäkringskassan ska även särskilt redogöra för huruvida myndigheten gjort en utvärdering av det egna informationssäkerhetsarbetet genom något analysverktyg, t.ex. Myndigheten för samhällsskydd och beredskaps verktyg Infosäkkollen, samt huruvida åtgärder vidtagits med anledning av resultatet.

Försäkringskassan har ett ledningssystem för säkerhet anpassat till standarden ISO/IEC 27001. Försäkringskassans Riktlinjer *Säkerhetsregler* fungerar som ramverk till ledningssystemet. Säkerhetsreglerna är baserade på krav utifrån ISO 27001, lagar, förordningar och föreskrifter. Under 2023 har Försäkringskassans säkerhetsregler omarbetats för att följa den nya strukturen i ISO 27001:2022. I samband med anpassningen till den nya standarden har nya säkerhetskrav beaktats, inarbetats och formats utifrån Försäkringskassans behov.
I den nya versionen av säkerhetsreglerna har informationsklassningsmodellen utvecklats för att förenkla för medarbetarna att informationsklassa information. I den nya informationsklassningsmodellen finns en tydligare koppling mellan konsekvensnivåerna och lagstiftning såsom exempelvis offentlighets- och sekretesslagen. Det väntas bland annat bidra till att förenkla sekretessprövningen vid utlämnade och underlätta i samverkan med andra myndigheter.
Säkerhetsreglerna har även uppdaterats och anpassats med anledning av förändrade externa krav inom områdena säkerhetsskydd, incidenthantering, beredskap och sektorsansvar.

Försäkringskassan har under det senaste året genomfört en översyn av hur säkerhetsarbetet är organiserat med ambitionen att uppnå en effektivare resursanvändning och öka förmågan att möta nuvarande- och kommande utmaningar. Förändringar i säkerhetsskyddslagen, uppdraget som sektorsansvarig myndighet och det försämrade omvärldsläget är också faktorer som legat till grund för översynen. En ny säkerhetsorganisation beslutades under våren 2023.

Säkerhetskultur och säkerhetsmedvetande hos medarbetare
Säkerhet ska vara en del av Försäkringskassans kultur. Varje medarbetare ska ha ett högt säkerhetsmedvetande och inse betydelsen av sin egen medverkan i ett effektivt skydd. Utöver säkerhetsutbildningen med det obligatoriska kunskapstestet som medarbetarna ska genomföra minst vartannat år så genomförs kompletterande utbildningar. Under det senaste året har lärarledda utbildningar genomförts där Försäkringskassans medarbetare har fått fördjupad kunskap inom flera säkerhetsområden, däribland informationssäkerhet.
Försäkringskassan har särskilda krav på att utbildningar ska genomföras för att få arbeta inom vissa områden. Exempel på områden är skyddade personuppgifter, säkerhetsskydd, signalskydd och säkerhet vid it-utveckling.

Under de senaste åren har den rättsliga styrningen och stödet stärkts med ett ökat antal jurister. Under det senaste året har det bland annat inrättats en rättsfunktion på IT-avdelningen som kommer att stödja avdelningen i rättsliga frågor som rör dataskydd och digitalisering. På Rättsavdelningen fortsätter arbetet med att uppdatera och utveckla styrningen inom bland annat dataskydd. Även arbetet med att uppdatera och utveckla utbildningarna inom dataskydd till Försäkringskassans personal fortsätter. Under år 2024 planeras beslut om en digitaliseringsvägledning för att ge stöd för medarbetare inom Försäkringskassan som arbetar med utveckling av digitala tjänster. Alla dessa insatser syftar till att öka kunskapen om, -och kapaciteten att följa berörda regelverk.

Genomförda och planerade insatser för att stärka informationssäkerhetsarbetet
Försäkringskassan har initierat ett pilotprojekt som handlar om att inrätta verksamhetsnära säkerhetsrådgivare för att säkerställa att det finns en utpekad samarbetspartner inom säkerhetsfrågor på alla avdelningar på Försäkringskassan. Detta är ett led i att utveckla stödet inom säkerhet i syfte att stärka avdelningarnas förmåga att analysera, utveckla och hantera uppkomna säkerhetsutmaningar för att kunna lösa sitt uppdrag både i ett komplext normalläge och i krig. Arbetet, som är i ett inledningsskede kommer att utvecklas löpande över året.

Försäkringskassan har genomfört ett antal åtgärder inom signalskyddsområdet. Åtgärderna har syftat till att anpassa signalskyddet efter verksamhetens behov. Dessa åtgärder har bland annat varit inom organisation, utrustning, lokaler med mera. Kompetensutveckling och personalförstärkning har bidragit till en ökad förståelse och ett mer ändamålsenligt signalskydds- och säkerhetsskyddsarbete. Utifrån omvärldsläget och Försäkringskassans uppdrag fortsätter myndigheten att aktivt arbeta med åtgärder för att göra områdena ännu mer ändamålsenliga utifrån verksamhetens behov.

Åtkomststyrning är en viktig del av Försäkringskassans informationssäkerhetsarbete. Hanteringen av åtkomststyrningen utvecklas kontinuerligt för att på bästa sätt skydda myndighetens informationstillgångar. Som ett led i utvecklingen av förbättrad åtkomststyrning har anpassade behörighetspaket inrättats. Behörighetspaket innebär att enskilda behörigheter samlas i beställningsbara paket. De nya behörighetspaketen innehåller olika behörigheter som är anpassade utifrån den anställdes arbetsuppgifter. Förändringen förväntas leda till att ytterligare säkerställa att medarbetare endast har de behörigheter de behöver för att utföra sitt arbete samt att administrationen av åtkomst effektiviseras för att ge ett bättre stöd till chefer.
Initiativ har även tagits för att ytterligare stärka Försäkringskassans operativa förmåga inom åtkomststyrning. Bland annat förbättras möjligheten att, på ett effektivt och säkert sätt administrera åtkomsträttigheter vid organisationsförändringar och omfördelning av personal. Arbete pågår även för att stärka förmågan att följa upp och kvalitetssäkra priviligierade åtkomsträttigheter ur ett ägarperspektiv.

Försäkringskassan utvecklar strategin mot otillåten påverkan, korruption och infiltration för att ytterligare säkerställa att informationstillgångarna säkras. Utvecklingen omfattar bland annat att identifiera vilka roller som löper större risk att utsättas för påtryckningar och infiltration, för att skapa bättre förutsättningar att anställa pålitlig och säkerhetsmedveten personal samt stärka befintlig personals motståndskraft. Detta kommer bland annat ske genom att utveckla rekryteringsprocessen samt systematisera utbildningsinsatser. Underlaget för att identifiera utsatta roller beräknas vara fastställt till sommaren 2024. Det vidare arbetet med att ta fram och utveckla säkerhetsåtgärder kommer ske löpande under året.
Försäkringskassan arbetar aktivt med att stävja otillåten informationssökning. Det görs bland annat genom kommunikationsinsatser och information till medarbetarna i syfte att förhindra dataintrång.

Försäkringskassan bedriver samhällsviktig verksamhet och har långtgående ansvar avseende den viktiga samhällsfunktionen att betala ut statliga ersättningar. Funktionen är nödvändig för samhällets grundläggande behov, värden och säkerhet. Försäkringskassan måste ha förmåga att administrera socialförsäkringen samt de övriga ersättningar som myndigheten förvaltar under svåra samhällsstörningar och ytterst under krig vilket ställer höga krav på informationssäkerhetsarbetet. Myndigheten måste även ha förmåga inom andra ansvarsområden som ligger utanför myndighetens grunduppdrag, såsom att säkerställa samordnad säker statlig it-drift. Under 2023 har Försäkringskassan bedrivit ett omfattande arbete via särskilt program, operativ förmåga vars syfte har varit att accelerera myndighetens arbete med att utveckla förmåga att upprätthålla verksamheten under svåra samhällsstörningar och ytterst krig. Utöver det

interna arbetet har flertal analyser och övningar genomförts med myndigheterna inom sektor ekonomisk säkerhet samt deltagande på övningar från Försvarsmakten och MSB.

Under 2024 kommer Försäkringskassan fortsätta arbetet med att stärka den operativa förmågan. Exempelvis inom områdena robust och säker kommunikation, cybersäkerhet och säkerställande av tillgång till verksamhetskritisk information.

Externa samarbeten som bidrar till förbättrad informationssäkerhet
Försäkringskassan har deltagit i samverkan på operativ nivå inom IT-säkerhetsarbetet genom att SOC-funktionen deltar i GovSec samverkansforum som drivs av MSB/CERT-SE. Syftet med GovSec är att på ett operativt plan inom cybersäkerhetsområdet utveckla ett effektivt samarbete för bättre incidenthantering, erfarenhetsutbyte, informationsdelning samt stärkt förtroende mellan forumets medlemmar.

Försäkringskassan deltar fortsatt i eSamverkansprogrammet där flera initiativ syftar till att stärka informationssäkerheten. Andra exempel där Försäkringskassan bidrar är arbetet med den förvaltningsgemensamma infrastruktur (ENA) och E-hälsomyndighetens uppdrag kring en sammanhållen intygshantering inom hälso- och sjukvård och omsorgen som båda bidrar med ökad informationssäkerhet och resiliens.

Försäkringskassan har ett nära samarbete med ett flertal andra myndigheter för att stärka robusthet och resiliens inom ramen för samordnad säker statlig it-drift.

Utvärdering av informationssäkerhetsarbetet
Försäkringskassans mål med rätt säkerhet innebär balans mellan att: kostnad och arbetsinsats för att efterleva säkerhetsreglerna är acceptabla, och att; incidenter inträffar med en allvarlighetsgrad och i en omfattning som kan tolereras. Balansen motsvarar Försäkringskassans riskaptit. Informationssäkerhet är en del av Försäkringskassans säkerhetsarbete.
Ett sätt att undersöka i vilken grad målet om rätt säkerhet har nåtts är genom att mäta efterlevnad av de beslutade säkerhetsreglerna. Försäkringskassans säkerhetsregler avser administrativa och tekniska säkerhetsåtgärder. Om de inte efterlevs i sin helhet går det heller inte att förvänta sig att incidenter enbart inträffar i en allvarlighetsgrad och i en omfattning som kan tolereras.
Försäkringskassan har tagit fram en mätmetod för efterlevnad av säkerhetsregler. Mätmetoden indikerar förbättringsområden genom nyckeltal där nivån av efterlevnad av säkerhetsreglerna visar i vilken omfattning Försäkringskassan exponeras för risker som är större än de risker som hanterats genom utformning av säkerhetsreglerna. Mätmetoden innehåller en skala med olika nivåer som efterlevnaden av säkerhetsreglerna bedöms utifrån. Med hjälp utav de olika nivåerna kan resultat beräknas på aggregerad nivå. Mätmetoden utgör ett viktigt verktyg för att identifiera förbättringsområden.

Under 2023 har en mätning av efterlevnaden av de interna it-säkerhetsanvisningarna genomförts via självskattning med hjälp av den nya mätmetoden. Skattningen bildar underlag till en analys där brister identifieras och förbättringsåtgärder utformas och prioriteras.
Som ett komplement till efterlevnadsskattningen har även ett arbetssätt utformas för att göra benchmarking av Försäkringskassans it-säkerhetsarbete gentemot det internationellt etablerade vägledningen CIS Critical Security Controls v8. Resultatet används i Försäkringskassans förbättringsarbete.

Utöver den framtagna mätmetoden så har Försäkringskassans genomfört MSB:s infosäkkollen som stöd för att utvärdera informationssäkerhetsarbetet. Frågeställningarna i infosäkkollen har utgjort ett bra stöd för att identifiera förbättringsområden inom informationssäkerhetsområdet. Frågeställningarna i

infosäkkollen har, tillsammans med andra analysverktyg bidragit till beslut om åtgärder för att stärka informationssäkerhetsområdet.

Vid genomförande av MSB:s uppföljning av informationssäkerhet och it-säkerhet, Infosäkkollen och it-säkerhetskollen för 2023 så har utvecklingsaktiviteter kopplat till ledningssystemet identifierats som bidrar till att nå Försäkringskassans säkerhetsmål. De identifierade aktiviteterna har lyfts i verksamhetsplanen för säkerhetsområdet. Dessa identifierade och planerade åtgärder redovisas övergripande enligt nedan.

Initiativ planeras för att utveckla och ytterligare stärka förmågan att identifiera och hantera verksamhetsrisker inom säkerhetsområdet. Försäkringskassan ser möjligheter att utveckla metoder och verktyg för att identifiera och hantera risker inom säkerhetsområdet vilket skulle bidra till en högre träffsäkerhet och kvalitet i riskbedömningarna.

Utifrån analysarbetet har en möjlighet till förbättring även identifierats inom incidentområdet. Försäkringskassan ser en möjlighet att förbättra det förebyggande säkerhetsarbetet genom att utveckla arbetet med orsaksanalyser av incidenter och stärka sambanden med risk och mätning. Förbättringsarbetet inom incidentområdet förväntas också bidra till en effektivare implementering att korrigerande och förebyggande åtgärder där hela verksamheten drar nytta av identifierade förbättringar. Det förväntas även bidra till en effektivare användning av resurser.

Beslut i detta ärende har fattats av generaldirektör Nils Öberg i närvaro av avdelningschef Stefan Blom och verksamhetsutvecklare Stefan Hultemar, den senare som föredragande.

Nils Öberg

Stefan Hultemar